AMENDMENT(S) TO THE SPECIFICATION:

Kindly amend paragraph [0067] on page 14 as follows:

--[0067] Note that while in one embodiment, the address indicates to the DMA controller 307 whether a DMA transfer is to or from the DMA engine 324 or the memory ~~interface313,~~ interface 313, in an alternate embodiment, a separate indication, e.g., a control bit is used to indicate whether a DMA transfer is to or from the DMA engine 324 or the memory ~~interface313.~~ interface 313.--

Kindly amend paragraph [0082] on page 17 as follows:

--[0082] The network DMA engine 324 interprets the information in the second special-type packets, i.e., in the streaming data encapsulating packets that contain the encapsulated information, encrypted in the case in-line encryption was included. One aspect is that the pointer and length information in the second-type-special packets is used to match the packet as a response to a DMA request. The network DMA engine 324 removes the data—possibly encrypted data— and communicates them via the bus 309 as responses to the matching DMA requests. To the host system bus, these appear as regular DMA responses transfers set up by the host DMA controller 307, since for such transfers, the network DMA ~~engine 328~~ engine 324 is set up as if it was a memory interface.--

Kindly amend paragraph [0092] on page 20 as follows:

--[0092] FIG. 4A shows another triplet 445 describing the integrity and key management used. In one embodiment, the information transmitted by the triplet 445 is also in the form of a pointer to the table in the switch that describes different methods. The first element ID_Integr 431 identifies the element as one for the integrity and/or authentication method, then a field 433 denoted ~~Length_ Integr~~ Length_Integr indicates the length of the integrity and/or authentication method data. The next field 435 is the pointer itself that points to the cryptographic integrity and/or authentication method in the key store 345. This identifies the integrity and/or authentication method to be used for the encryption (or decryption in the case of receiving).--

Kindly amend paragraph [00107] on page 23 as follows:

--[00107] Thus, for the transmit path, the AP 300 generates the memory request. The smart DMA engine 324 includes ~~signalling~~ signaling methods to pass the cryptographic details in the form of the additional triplets. In one embodiment, these are as described above and convey a pointer or pointers to the key store 345. In another embodiment, the cryptographic information includes triplets for one or more pointers to where the cryptographic information is stored in the memory of the switch 335. In yet another embodiment, the cryptographic information, in the form pointer or pointers to the key store 345, are maintained in the local host memory 315 of the AP, and of the values of the pointers are encapsulated as triplets for the ~~cryptogrpahic~~ cryptographic information by the network DMA engine when forming the special packets of the first kind to

initiate a streaming network DMA request. Thus, the additional cryptographic information in the additional type/length/value triplets are added to the request. The filter 337 in the switch recognizes packets of the special type and sets up the network packet and DMA engine 338 to carry out the DMA transfer from the switch memory. Furthermore, using the additional type/length/value triplets for cryptography, in response to the network packet the DMA engine also sets up the cryptography engine 321 to encrypt as requested according to information stored in the key store 345.--

Kindly amend paragraph [00117] on pages 24 and 25 as follows:

--[00117] The DMA request from the host DMA controller 307 is translated by the network DMA engine 324 to a packet of the second special type that includes the pointer and length data for the transfer, and the data element of the transfer to be written into the switch memory. Furthermore, the cryptographic information needed to decrypt the packet is also included in the form of additional triplets. The packet of the second type, including the cryptographic information, is sent to the switch 329 via the network via the Ethernet MAC and PHY interface and the network ~~link 327.~~ link 328.--